Acht antiviruspakketten getest

Voel je veilig!

Het gaat van kwaad naar erger met de computervirussen en aanverwante ondingen. Nieuwe virussen verspreiden zich kennelijk zowat met de snelheid van het licht. Zelf ben je natuurlijk een open doel voor dat soort vandalen. Antivirussoftware moet je daartegen beschermen. En wij zijn er om te kijken of die bescherming ook wel doet wat de reclame belooft.

Echt nieuws is het wellicht niet meer als je leest of hoort dat er alweer een beveiligingslek ontdekt is in Windows of één van de standaard meegeleverde programma's. Het lijkt wel alsof elk nieuw virus geen enkele moeite heeft om een willekeurige pc te besmetten. En Microsoft lijkt niet in staat Windows behoorlijk te beveiligen. Hier speelt natuurlijk mee dat hackers en virusauteurs zich bijna exclusief op Windows richten, omdat dat nu eenmaal het meest gebruikte systeem is. Gelukkig is er software die je helpt Windows dicht te timmeren. Antivirussoftware speelt hierin een belangrijke rol. Helaas loopt zulke software per definitie achter op de prestaties van de virusmakers. Zo moet een nieuw virus eerst pc's besmet hebben voordat de antivirusspecialisten aan het werk kunnen om er een remedie voor te bedenken.

De test

We onderzochten acht antivirusproducten. Bij dit artikel hoort een tabel. Bovenaan vind je productinformatie en daarin zie je onder meer wat voor opties voorzien zijn. Om te kijken hoe goed de programma's zijn in het opsporen van virussen, organiseerden we een detectietest. De resultaten daarvan vind je onderaan de tabel. We hebben zelf een viruscollectie samengesteld van virussen die al ooit in onze contreien voorkwamen, of toch zoveel mogelijk. In totaal zitten er 17.441 virussen in onze collectie. Maar bedenk dat er terwijl we dit schrijven volgens Symantec [www.symantec.com] zo'n 65.135 virussen bestaan. In onze collectie is de overgrote meerderheid van het COM-type (13.957 stuks): dit zijn niet de nieuwste, maar wel nog steeds voorkomende virussen. Voorts hebben we 3.232 exe-bestanden met een virus aan boord en daar zitten wel nieuwe bij, onder meer beestjes zoals Nimda en het beruchte CIH-virus. Macrovirussen zijn natuurlijk ook belangrijk. Er zijn er duizenden, maar je kan ze onderverdelen in enkele tientallen hoofdgroepen. Wij hebben uit elke hoofdgroep één of meer macrovirussen in ons testbestand zitten. Momenteel hebben we 243 verschillende macrovirussen. Om het wat vollediger te maken hebben we ook nog negen bestanden met niet door de gebruiker uitvoerbare binaire bestanden (zoals OBJ- en DLL-bestanden, VXD-drivers voor Windows, startsectordata enzovoorts). We noteerden hoeveel virussen van iedere soort elk antivirusproduct herkende en drukten het totaal uit als een percentage. Helaas bleek geen enkele scanner in staat ze allemaal te herkennen, zelfs de meest recente niet.



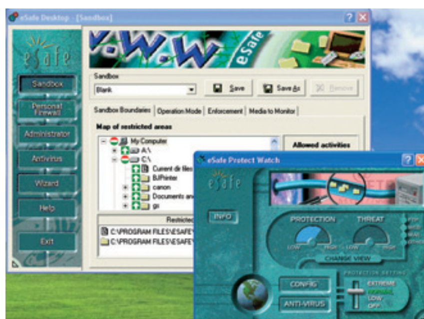
ANTIVIRUSSOFTWARE: EEN WONDERMIDDEL TEGEN GRIEP





eSafe Desktop

eSafe Desktop houdt vrij letterlijk álles in de gaten. Heel aardig is dat het binnengehaalde programma's in feite niet blokkeert, maar onder strikt toezicht (in een zogenaamde softwarezandbak) uitvoert om te kijken of ze zich als vandalen gedragen. Zo ja, dan grijpt eSafe Desktop in voordat zulke software of applicaties wat ergs kunnen doen. Dit beperkt je mogelijkheden als gebruiker niet (in tegenstelling tot andere soorten van preventiesoftware) en vangt toch alle mogelijke vandalenstreken op. Een probleem is wel de juiste afstelling van deze preventie. Als je de beveiliging hoog zet en niet aanpast, krijg je namelijk om de haverklap waarschuwingsvenstertjes en het is niet leuk om zo te werken. Een goed evenwicht vinden tussen beveiliging en werkbaarheid is dus de boodschap. De eigenlijke virusscanner blijkt echter vrij zwak en detecteert ronduit slecht. Schoonmaken van besmette bestanden is zelfs vrijwel onbestaande. Als je die zandbak aan hebt staan, is dat echter niet eens zo belangrijk. Alle door de scanner gemiste virussen werden namelijk keurig afgeblokt toen ze probeerden ons testsysteem te infiltreren. Verder kan je zelf uitgebreid opgeven wat voor data op je systeem zeker nooit het internet op mag en je al dan niet laten waarschuwen als iets of iemand dat toch probeert. Ten slotte zit er ook nog een persoonlijke *firewall* in. Als je écht veilig wil surfen, kan je wat ons betreft nauwelijks buiten zo'n gecombineerd systeem met zandbak en firewall. Vroeger kon je eSafe gratis downloaden en gebruiken, maar dat is niet langer zo. Je kan het nog wel downloaden, maar dat is een evaluatieversie en na dertig dagen is het afdokken of kinkloppen. En het is niet goedkoop! Je kan het overigens ook on line kopen bij [**www.esafe-desktop.com**].

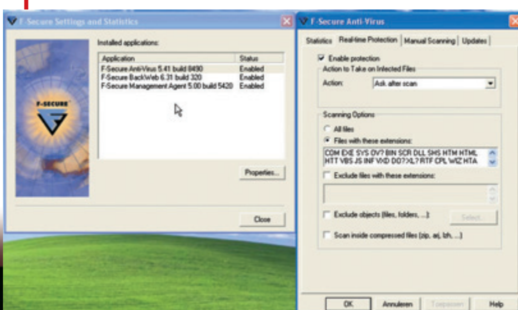


eSafe: vooral handig dankzij de zandbakfunctie.

F-Secure Internet Security Suite 2003



F-Secure Anti-Virus (FSAV) komt uit Finland. Het is minstens zo oud als de McAfee virusscanner. Net zoals bij de andere software in deze test draait er bij wijze van preventie een permanente achtergrondtaak in Windows die je systeem in de gaten houdt. Je kan de eigenlijke detector manueel of geautomatiseerd starten. Voor dat laatste is er een op takenbeheer gesteunde interface. Hierbij maak je uit te voeren taken aan, waarbij je aangeeft wat er moet gebeuren, wanneer en hoe. Er zijn al een aantal voorbeeldtaken aanwezig die je kan gebruiken als model, maar je mag ook volledig van de grond af een taak opbouwen. Updates haal je met een druk op de knop van het internet, maar het gaat niet zo makkelijk als bij sommige andere pakketten. Interessant: bij inspectie van de updates bleken die afkomstig te zijn van het Kaspersky Lab in Rusland en daar komt ook het AVP-pakket vandaan. FSAV vond van de door ons voorgelegde virussen het grootste aantal en blonk vooral uit in het vinden van macrovirussen en in binaire, niet-rechtstreeks-uitvoerbare bestanden verstopte virussen.



F-Secure AntiVirus: blinkt uit in macrovirussen.

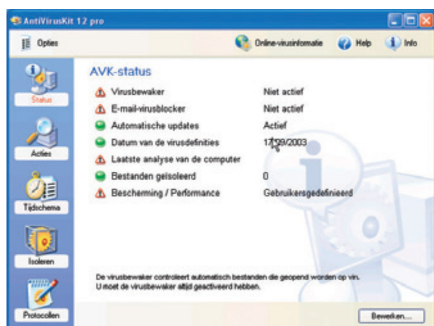
VAKTAAL

Firewall: Een veiligheidsvoorziening die de gegevensuitwisseling in het oog houdt. Wie zich op het internet begeeft, kan zich op die manier beschermen tegen personen die zonder toestemming zijn systeem binnendringen.

G-Data AntiVirusKit 12 Pro



Het Duitse G-Data is een nieuwe speler op de markt van de antivirussoftware en wordt in de Benelux verdeeld door het Nederlandse Denda. Die hebben zich wel moeite getroost, want het hele pakket (verpakking, handleidingen en de software) gebruikt keurig Nederlands. Gewoonlijk staan we erg sceptisch tegenover nieuwelingen op de antivirusmarkt, gewoon omdat het zo beestig moeilijk is een nieuwe antivirusengine te schrijven. G-Data besefte dat kennelijk ook, want zij gebruiken die van een succesvolle derde: Kaspersky. Daarnaast gebruikt AntiVirusKit nog een tweede engine: RAV. Dat belooft dus voor de prestatietest. Qua interface zijn we echt in de wolken: het ziet er prachtig, maar toch overzichtelijk uit met hele mooie grote pictogrammen voor het hoofdmenu aan de linkerkant van het dialoogscherm. Alles wat ons hartje maar begeert is voorzien. Zoals we verwachtten scoort AntiVirusKit prima in onze testen. Wel verwonderde het ons dat de scanner ondanks de twee engines (waaronder die van Kaspersky) toch minder virussen vond dan het product van Kaspersky zelf. We hebben uiteraard voor elk product voorafgaand aan de test een update laten uitvoeren van de virusinformatie en indien mogelijk ook van de software zelf. Het waarom van deze afwijking is voor ons dan ook een raadsel.

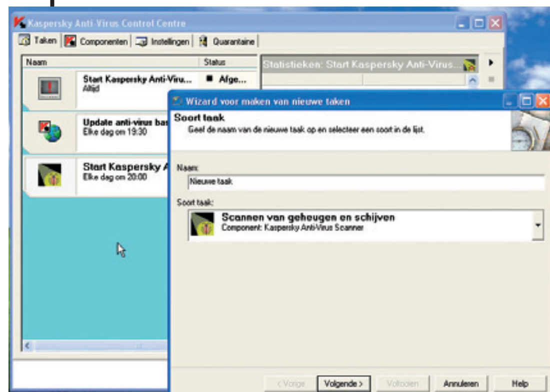


G-Data AntiVirusKit 12 Pro: twee antivirus-engines.

Kaspersky Personal Anti-Virus



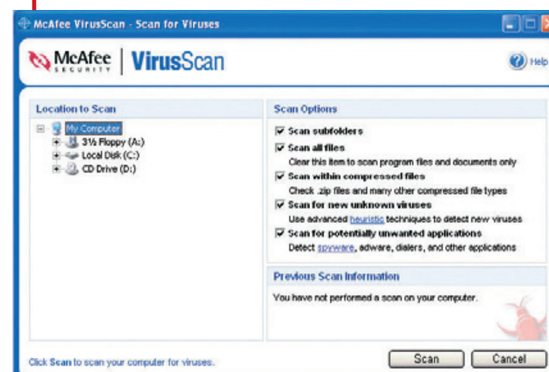
Het Russische AVP-pakket van Kaspersky Labs krijgt wereldwijd steeds meer aandacht. Zelfs het Finse F-Secure en nog andere producenten maken gebruik van de antivirusinformatie van Kaspersky. We moeten echt zeggen dat we onder de indruk zijn. Dit pakket doet zowat alles, maar het heeft geen zandbakfunctie zoals eSafe Desktop of Norman voor het afschermen van allerlei kwaadaardig spul. De preventie bestaat uit het in de achtergrond uitvoeren van scans en een paar basismaatregelen. De detectie is heel erg goed en vecht in onze testen meestal nek-aan-nek met die van F-Secure. We zien AVP wel zitten omdat het voor zowat elk besturingssysteem te vinden is en er allerlei andere beveiligingsmaatregelen te verkrijgen zijn bij de Benelux-leverancier Kaspersky Lab in Nederland. AVP kost heel wat minder dan de concurrentie (F-Secure is zelfs het duurst van allemaal). Van AVP kan je een aantal verschillende versies krijgen: een Lite, een Personal en een Personal Pro versie. De verschillen daartussen hebben te maken met wat je ermee kan beschermen en wat het pakket nog meer kan. Hoe meer het kan, hoe meer het kost – maar dat zal je wel niet verbazen.



Kaspersky Personal Anti-Virus: het beste op de markt.

NAI McAfee VirusScan 8

De nieuwste antivirustelg van Network Associates is McAfee versie 8 (je vindt het wel pas begin 2004 in de winkel!). Eventueel kan je die nog uitbreiden met een persoonlijke firewall, privacy-bescherming en een *spam*-filter. Die worden dan allemaal bediend vanuit de Security Console. Zoals vanouds heten de belangrijkste antiviruselementen VirusScan (de eigenlijke detector) en ActiveShield (achtergrondpreventie). Al die losse onderdelen worden allemaal keurig samen geïnstalleerd en je merkt er eigenlijk weinig van dat een en ander oorspronkelijk allemaal

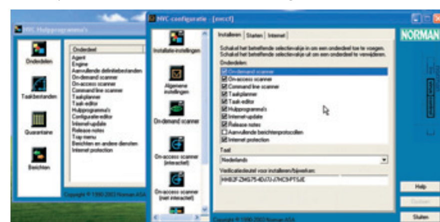


NAI McAfee VirusScanner: de beste schoonmaker.

Norman Security Suite



De Norman Security Suite omvat naast het antivirusprogramma ook nog een persoonlijke firewall en encryptiesoftware. De antivirusmaatregelen bestaan uit een 'on-demand' scanner (die je dus manueel of geautomatiseerd start om doelwitten te onderzoeken op virusinfecties) en een interactieve en een niet-interactieve 'on-access' scanner (die draait in de achtergrond en elk bestand onderzoekt dat geopend of vanuit het internet op het systeem geplaatst wordt). Bij de 'on-demand' scanner blijkt het niet mogelijk om een virusinfectie volautomatisch te laten repareren: het programma toont eerst een lijst van gevonden infecties en daarna moet je op een knop 'Opschonen' klikken voordat hij met de reparatiefase begint. Vanaf versie 5.5 doet bij Norman de zandbak de intrede. Norman grijpt bij het gebruik van hun zandbak niet zover in het systeem in als eSafe, maar het dient in elk geval ook om routines in uitvoering te kunnen bewaken en onmiddellijk in te grijpen als die iets mispeuteren. Wij konden bij het systeem van Norman geen nadelen in prestaties of beperkingen in ons desktopgebruik vaststellen, maar je mag dus niet de fout maken te veronderstellen dat dit zandbaksysteem je tegen alle virussen zal beschermen. We vinden het trouwens een nadeel dat de Norman zandbak zich beperkt tot binaire uitvoerbare bestanden en geen macro's of scripts kan evalueren. NVC neemt helaas de instellingen van IE niet over. Als bij je internetprovider het gebruik van een *proxyserver* bijvoorbeeld vereist is, lukt de updateprocedure niet. Die kan je wel manueel instellen, maar het is net ietsje gebruikersvriendelijker als je dat gewoon kon overnemen.


Norman Virus Control: nu ook met zandbak.



aparte software was. Bovenop al deze deelsoftware zit de eerder genoemde Security Console, een bedieningsconsole voor alle beveiligingsgerelateerde software van McAfee. Net als bij andere scanners in deze test configureer je onmiddellijk of later uit te voeren taken met behulp van een wizard. NAI brengt minstens eenmaal per maand een nieuwe versie van de virusdatabase uit. Je kan die mits een wachtwoord van hun website halen. Het automatisch aftasten van materiaal dat van het internet komt is keurig voorzien en alle bewaaracties worden sowieso gecontroleerd via ActiveShield. VirusScan 8 blijkt het beste te zijn in het schoonmaken van gevonden virussen. De detectie is goed, maar niet de beste.

Preventie!

Virusdetectie is niet genoeg. Een scanner vindt namelijk alleen maar virussen die al bekend zijn. Als er dan een virus op je systeem komt dat nog niet bekend is, kan dat vrijelijk zijn gang gaan en heel wat schade aanrichten. Ga er dus van uit dat een scanner nooit alle virussen kan vinden en dat er dus altijd wel door de mazen van het net glippen. Dat blijkt ook uit onze detectietest: van de meer dan 17.000 virussen die we voorlegden aan de scanners bleken zelfs de allerbeste er meerdere tientallen niet te vinden. En het gaat over bekende virussen! Reden te over dus om geen blind vertrouwen te hebben in antivirussoftware. Een scanner helpt je om bekende virussen te detecteren, maar je hebt dus nood aan maatregelen die een virus verhinderen zijn vuile werk te doen. We plaatsen al die maatregelen onder de noemer preventie. Goede preventie zorgt ervoor dat een onbekend virus je systeem niet kan infecteren, of zich althans niet kan voortplanten. Zelf moet je natuurlijk ook een paar dingen doen en laten. Voer dus programma's die je van anderen krijgt nooit zomaar uit en lees documenten ook nooit zomaar in. Eerst even een virusscan uitvoeren is de boodschap. Alles wat je van het internet haalt of wat via e-mail al dan niet ongevraagd naar je toe wordt gestuurd is natuurlijk per definitie verdacht. Klik NOOIT op aanhangsels! ActiveX en VB-scripts zijn erg goede manieren om virussen in je systeem te smokkelen. Uitschakelen dus of tenminste software draaien die dergelijke applets in de gaten kan houden.

VAKTAAL

Proxy(server): Een computer bij je internetprovider die in feite als een tussenstation fungeert tussen je eigen pc en de computer op het internet waar je een webpagina wil opvragen. Blijkt de webpagina die je hebt aangevraagd zich al op die speciale proxyserver te bevinden, dan krijg je die pagina van daaruit aangereikt en dat gaat natuurlijk een stukje sneller.

Spam: Hiermee worden de ongevraagde e-mailberichten aangeduid die in je mailbox terecht komen.

Panda AntiVirus Titanium

Panda Software uit Spanje heeft verschillende antivirusproducten, maar wij bekijken alleen de versie voor alleenstaand desktopgebruik. Qua mogelijkheden en gebruiksgemak lijkt het erg op de Amerikaanse concurrentie. Wat het Panda-pakket er echt met kop en schouders doet bovenuit steken is het niveau van de ondersteuning. Panda Software brengt dagelijks een update van de virusdatabase uit en ook de software zelf wordt zeer regelmatig bijgewerkt. Al deze updates kunnen gratis van het internet gehaald worden, mits je je registratiekaart instuurt, want dan pas krijg je het wachtwoord dat je daarvoor nodig hebt. Heel interessant: Panda verkondigt dat als jij een door hun software niet herkend virus tegenkomt, je hen mag contacteren en zij garanderen dan binnen de vierentwintig uur een nieuwe versie van de antivirussoftware die dat virus wél kent en kan onderscheppen. We hebben dat eens uitgeprobeerd: we stuurden zes van de bestanden die hun scanner niet detecteerde naar Panda Software om te kijken wat zij ermee zouden doen. De volgende dag kregen we een nieuwe versie van de virusinformatiedatabase die de zes door ons doorgegeven virussen niet alleen herkende, maar specifiek bij naam noemde. Dat laatste toont ons dat men bij Panda serieus onderzoek gedaan heeft naar de nieuwe virussen en niet gewoon klakkeloos een paar nieuwe signaturen in de database bijgevoegd heeft. Een eigenaardigheidje kwamen we tegen bij de installatie van de Titanium-versie: je moet op een gegeven moment een gebruikersnaam invullen en verplicht ook een bedrijfsnaam. Dat moet dus ook als je een particulier bent, want anders blijft de 'volgende'-knop uitgegrijsd en kan je dus niet verder met de installatie.

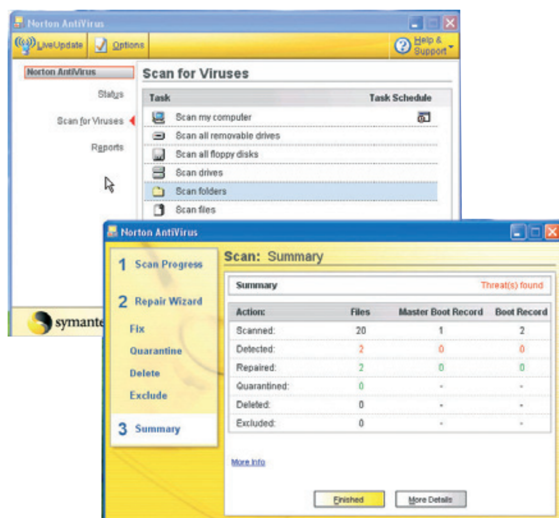


Panda Antivirus Titanium: dagelijkse updates.



Symantec Norton AntiVirus 2004

Symantec is het kennelijk beu dat zijn antivirussoftware een van de vaakst gekopieerde is en voert vanaf Norton AntiVirus 2004 een activatiesysteem in in de internationale versie, ongeveer zoals Microsoft dat heeft. We kunnen natuurlijk niet anders dan ons afvragen hoe lang het zal duren eer ook dat gekraakt wordt (net zoals dat van Microsoft), maar het zit er nu in elk geval in. De Nederlandstalige versie blijft voorlopig nog gespaard van een activatiesysteem. Net zoals bij veel concurrenten is de centrale interface van Norton AntiVirus een soort van takenbeheer. Het geheel is erg gebruiksvriendelijk en we vinden het hele bedieningssysteem een voorbeeld voor alle andere producenten. Zo moet het! De 'LiveUpdate'-knop is ook nog steeds een voorbeeld voor alle andere softwareproducenten en heus niet alleen die van antivirussoftware. Overigens kan je met LiveUpdate alle producten van Symantec op je systeem updaten, niet alleen het antivirusprogramma. Inzake preventie controleert Norton AntiVirus alle wijzigingsoperaties op je harde schijf. Alles wat niet is zoals het hoort en met name als iets probeert bestanden te wijzigen of te wissen waar dat niet zou mogen, blokkeert hij en geeft dan een waarschuwingsvenster. Norton AntiVirus blijkt niet zo goed in het repareren van besmette bestanden. Zorg dus altijd voor een gegarandeerd virusvrije back-up van je systeem als je dit product gebruikt, want je kan niet echt vertrouwen op de schoonmaakfaciliteiten.



Symantec Norton Antivirus 2004: erg gebruiksvriendelijk.



Meer informatie over deze antiviruspakketten vind je on line op [www.clickxmagazine.be]











Merk Productnaam	eSafe Desktop	F-Secure Internet Security 2003	G-Data AntiVirusKit 12 Pro	Kaspersky Personal Anti-Virus	NAI McAfee VirusScan	Norman Security Suite	Panda AntiVirus Titanium	Symantec Norton Anti-Virus 2004
Merk website	www.esafe-desktop.com	www.f-secure.com	www.kas-persky.com	www.kas-persky.com	www.mcafee.com	www.norman.com	www.panda software.com	www.symantec.com
Commerciële Info								
Adviesprijs	€ 99,22	€ 78,65	€ 29,95	€ 32	€ 54,39	€ 49,01	€ 31,46	€ 55,93
Leverancier	Microcraft	Data Rescue	Denda Multi media bv, NL	Kaspersky Lab Benelux	Tech Data / Ingram Micro	Norman Belgium	Panda Software NV	Symantec Belgium
Telefoon	019/63.22.92	04/344.65.10	0031 54/ 157.02.70	0031 73/ 615.48.60	02/583.83.24 / 02/254.92.11	089/24.37.04	02/756.08.80	02/531.11.40
Leverancier - website	www.microcraft.be	www.datarescue.be	www.denda.com	www.kasperskylab.nl	www.tech-data.be / ingrammicro.be	www.norman.nl	www.panda-software.be	www.syman-tec.com
Technische Informatie								
Evaluatieversie downloadbaar?	Ja	Ja	Nee	Ja	Ja	Ja	Ja	Ja: US-versie!
Bescherming tegen infecties vanaf het internet?	Ja (totaal)	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Gratis software-updates	Ja	Nee	Ja (registratie)	Ja (registratie)	Ja (registratie)	Ja	Ja (registratie)	Ja
Gratis virusdatabase update via internet?	Ja	Ja	Ja (registratie)	Ja (registratie)	Ja (registratie)	Ja	Ja (registratie)	Ja
Preventiemaatregelen tegen infecties?	Beveiligde omgeving	Ja	Ja	Ja	Ja	Beveiligde omgeving	Ja	Ja
Virusverwijdering?	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Gepland automatisch starten van detectie?	Ja	Nee	Ja	Ja	Ja	Ja	Ja	Ja
Aanmaak noodstartdiskette/cd?	Ja	Nee	Ja	Ja	Ja	Ja	Ja	Ja
Persoonlijke firewall?	Ja	Ja	Nee	Nee	Nee: optie	Ja	Ja	Nee
Standaardduur ondersteuning en dienstverlening na aankoop?	1 jaar	1 jaar	1 jaar	1 jaar	1 jaar	1 jaar	1 jaar	1 jaar
Beoordeling								
Functionaliteitsscore (%)	85	67	42	55	50	82	65	53
Detectiescore (%)	95	95	94	95	92	93	92	93
Schoonmaakscore*1 (%)	0	80	76	77	82	46	76	57
Prestatiescore (totaal, op 100)	**51**	**84**	**78**	**81**	**82**	**71**	**81**	**71**
Prijsscore*2 (op 100)	24	31	81	81	44	49	49	43
Prijs/Prestatiescore*3	**38**	**58**	**80**	**81**	**63**	**60**	**65**	**57**

*1 Het percentage van alle virussen dat het programma van de besmette pc heeft kunnen verwijderen *2 Ideale prijs: 320 *3 50% prijs, 50% prestatie

Paniek zaaien

Geregeld verschijnen allerlei berichten over nieuwe virussen. Hoe weet je nu wat daarvan echt is? Er bestaan goede webpagina's hierover. Je kan een blik werpen op de Computer Virus Myths Homepage, [www.vmyths.com], waar je meteen ziet of een bericht een verzinsel is. Informatie over de laatste nieuwe echte virussen is te vinden op de websites van de meeste antivirussoftwareproducenten. Een andere mogelijkheid is de WildList [www.wildlist.org]: dat is een lijst van virussen die werkelijk pc's geïnfecteerd hebben en gerapporteerd werden door virushulporganisaties wereldwijd.

CONCLUSIE

De beste prijs/prestatieverhouding krijg je van Kaspersky Personal AntiVirus en op de tweede plaats van G-Data AntiVirusKit 12 Pro. De toppresteerder is nog altijd F-Secure AntiVirus, maar dat is dus wel peperduur. Gelukkig is ook het goedkopere NAI McAfee een toppresteerder.



– Johan Zwiekhorst –